L'invention concerne un procédé de communication sécurisé entre deux entités connectées à un réseau de type Internet.

Elle s'applique plus particulièrement à des communications via un réseau de type Internet comprenant un segment de transmissions sans fil.

L'invention concerne encore une architecture de système de communication pour la mise en œuvre de ce procédé.

Dans le cadre de l'invention, le terme "entité" doit être entendu dans son sens le plus général. Il s'agit aussi bien de ressources informatiques, matérielles ou logicielles, que, selon une caractéristique de l'invention qui sera explicitée ci-après, d'êtres humains, utilisateurs d'un des composants du système de communication.

Le terme "Internet" doit également être compris dans son sens le plus général. Il englobe, outre le réseau Internet proprement dit, les réseaux privés d'entreprises ou similaires, du type dit "intranet", et les réseaux les prolongeant vers l'extérieur, du type dit "extranet", de façon générale tout réseau dans lequel les échanges de données s'effectuent selon un protocole du type Internet. Cependant, pour fixer les idées, sans que cela limite en quoi que ce soit la portée de l'invention, on se placera ci-après dans le cas du réseau Internet proprement dit, sauf mention contraire.

Habituellement, les communications sur les réseaux, quelle qu'en soit la nature, s'effectuent conformément à des protocoles répondant à des standards comprenant plusieurs couches logicielles superposées.

L'architecture des réseaux de communication est décrite par diverses couches logiques. A titre d'exemple, le standard "OSI" ("Open System Interconnection"), défini par l' "ISO", comporte sept couches qui vont des couches dites basses (par exemple la couche dite "physique" qui concerne le support de transmission physique) aux couches dites hautes (par exemple la couche dite d' "application"), en passant par des couches intermédiaires, notamment la couche dite de "transport". Une couche donnée offre ses services à la couche qui lui est immédiatement supérieure et requiert de la couche qui lui immédiatement inférieure d'autres services, via des interfaces appropriées. Les couches communiquent à l'aide de primitives. Elles peuvent également

communiquer avec des couches de même niveau. Dans certaines architectures, l'une ou l'autre de ces couches peuvent être inexistantes.

Dans le cas d'un réseau de type Internet, les communications s'effectuent selon des protocoles, spécifiques à ce type de communications, mais qui comprennent également plusieurs couches logicielles. Les couches sont au nombre de cinq, et de façon plus précise, en allant de la couche supérieure à la couche inférieure : la couche d'application ("http", "ftp", "e-mail", etc.), la couche de transport ("TCP"), la couche d'adressage de réseau ("IP"), la couche de liens de données ("PPP", "Slip", etc.) et la couche physique. Le protocole de communication est choisi en fonction de l'application plus particulièrement visée : interrogation de pages "WEB" ("HTTP"), transferts de fichiers "FTP"), courrier électronique (e-mel, ou "e-mail" selon la terminologie anglo-saxonne), forums ou "news", etc.

Dans sa globalité, un réseau de type Internet comprend tout d'abord un ou plusieurs réseaux de transmission de données proprement dits, éventuellement divisés en sous-réseaux. Ces réseaux comprennent notamment des canaux de liaison physique qui constituent le niveau le plus bas. Les communications peuvent être assurées par des liaisons à relativement bas débit : liaisons téléphoniques, ou des liaisons à haut ou très haut débit : fibres optiques, faisceaux hertziens, liaisons satellites, notamment pour les artères principales. A ce ou ces réseau(x) sont connectés de nombreux systèmes, sous-systèmes, machines et/ou terminaux divers. La connexion peut être directe (à l'aide d'un modem, par exemple) ou indirecte, par l'intermédiaire d'un système dit "fire-wall" (ou "pare-feu"), d'un "proxy", ou par l'intermédiaire du système informatique d'un fournisseur d'accès au réseau Internet (ou "ISP" selon la terminologie anglo-saxonne).

La gamme des entités connectées, dans l'art connu, peut aller des ordinateurs très puissants (par exemple du type dit "main-frame") jusqu'à des terminaux "légers", c'est-à-dire ne possédant que peu de ressources informatiques propres, par exemple des terminaux dédiés, voire de simples terminaux lecteurs de carte à puce. Ces entités, que l'on peut appeler de façon générique "systèmes", disposent d'un système d'exploitation (ou "OS" selon la

terminologie anglo-saxonne), d'un type dit propriétaire ou non. A titre d'exemple, on peut citer le système d'exploitation "UNIX" (marque déposée"), très utilisé dans le cadre des applications relatives au réseau Internet.

Généralement, les communications entre entités connectées s'effectuent selon un mode dit client-serveur et mettent en œuvre la technologie dite d'objets. Un serveur peut être défini comme étant un logiciel, une application ou toute entité logicielle rendant un service donné (par exemple le transfert d'un fichier requis). Une telle entité est hébergée par des systèmes connectés au réseau Internet, que l'on appelle "serveurs". Une entité "client" peut être définie comme étant le dual de l'entité "serveur", c'est-à-dire demandant un service déterminé. Cependant, rien ne s'oppose à ce qu'un système ou une application soit à la fois "client" et "serveur".

Comme il a été indiqué, une des couches logicielle de communication est constituée par la couche d'adressage dite "IP". Il est en effet nécessaire qu'un client, par exemple, puisse adresser sélectivement un serveur, via le réseau Internet. Pour ce faire, la technologie Internet met en œuvre le concept dit d' "URL" (pour "Uniform Resource Locator") faisant appel à une adresse appelée "IP" (pour "Internet protocol"). Le réseau Internet est fortement hiérarchisé en domaines et sous-domaines, qui correspondent eux-mêmes à des réseaux et sous-réseaux, gérés par des système d'annuaires électroniques, dénommés "DNS" (pour "Domains Name Servers"). La structure de l'adresse "IP" reflète cette hiérarchisation. Elle comprend une adresse "IP" proprement dite, comprenant elle-même une adresse de sous-réseau appelée et une adresse d'une entité à l'intérieur de ce sous-réseau. Elle est associée à un numéro de port permettant d'adresser un serveur à l'intérieur de l'entité précitée.

Pour une même entité connectée au réseau Internet, les adresses "IP" peuvent être permanentes ou variables dans le temps. A titre d'exemple, les systèmes connectés au réseau Internet, via un fournisseur d'accès, se voient généralement attribuer une adresse différente au début de chaque session.

Dans une période récente, un certain nombre de besoins se sont fait sentir.

Un premier besoin concerne la mobilité. On parle de "nomadisme" des utilisateurs. Ceux-ci disposant de terminaux eux-mêmes mobiles, tels des micro-ordinateurs portables, ils désirent pouvoir se connecter à n'importe quel endroit du réseau, sans contraintes excessives. Notamment, la migration d'un domaine à un autre devrait être transparente pour l'usager. Il doit également pouvoir conserver son environnement habituel, par exemple conserver un accès à une liste de services auxquels il est abonné, gratuitement ou non, à un carnet d'adresses, etc. Les données caractérisant cet environnement peuvent être stockées dans un serveur éloigné auquel l'abonné peut accéder. Il peut encore les transporter avec lui, par exemple dans la mémoire d'une carte à puce.

Plus récemment, il a été proposé de connecter directement des téléphones mobiles, seuls ou combinés avec des appareils du type organiseur ou similaire, au réseau Internet. Cette connexion s'effectue physiquement par l'intermédiaire d'un réseau de transmissions sans fil, tel le réseau à la norme "Global System for Mobile communications (acronyme de "GSM"). Ce réseau est lui-même connecté au réseau Internet par l'intermédiaire de passerelles spécialisées ou "gateway" selon la dénomination anglo-saxonne.

Cette disposition est très avantageuse, car elle autorise une mobilité extrême. Il n'est plus nécessaire de disposer de points fixes pour se connecter au réseau Internet. *A priori*, la seule limite à cette mobilité résulte de la couverture territoriale, plus ou moins étendue, du réseau "GSM" d'un opérateur donné.

Cependant, il existe d'autres types de limitations dues à ce mode de transmission.

Une première limitation est relative à la bande passante. Dans l'état actuel des technologies, la vitesse de transmission est très faible : 9600 bits/s. Même dans le cas d'une simple ligne téléphonique filaire classique, la norme V90, par exemple, permet d'atteindre une vitesse maximale de 56000 bits/s. On peut obtenir des vitesses bien plus élevées si on fait appel à la technologie "ADSL" (470 kits/s à 1 Mbits/s). En outre, les liaisons de type "RNIS", par câble ou satellites permettent de hauts ou très hauts débits. De nouvelles technologies sont en cours d'étude ou d'implantation, telle "GPRS"

("Global Packet Radio Service") ou "UTMS" ("Universal Mobile Telecommunication Service") et autoriseront de plus grandes vitesses de transmission, mais ne sont pas encore toutes opérationnelles. Pour le moins, le réseau "GSM", dans sa version actuelle, subsistera pendant un laps de temps indéterminé, car des modifications et/ou des changements complets de matériels s'avéreront nécessaires, ce sera le cas notamment pour la version dite "G3" de "GSM"".

Une deuxième limitation, corollaire de la miniaturisation des dispositifs de communication sans fil, tient à la surface réduite, voire très réduite des écrans de visualisation de ces dispositifs.

Il s'ensuit que les protocoles Internet, notamment en ce qui concerne le "WEB" proprement dit (protocole "HTTP") ne sont pas adaptés. En particulier, le langage couramment utilisé pour ces applications est un langage interprété de description de pages, dit "HTML" ("HyperText Markup Language"), ce langage ne convient pas aux types d'écrans précités.

Aussi, il a été proposé un nouveau protocole, dérivé des protocoles de type Internet, de type propriétaire, appelé "WAP" pour "Wireless Application Protocol". Ce protocole permet, à des téléphones mobiles d'accéder à des applications de type "e-mail", "WEB" ou multimédia (vidéo par exemple), en tenant compte des caractéristiques spécifiques de ces appareils et du réseau de communication auquel ils sont connectés (par exemple le réseau "GSM").

Même si elle permet l'accès aux applications ci-dessus, cette solution n'est pas sans inconvénients.

Les sites Internet doivent être adaptés, car il n'est pas possible d'afficher sur l'écran d'un téléphone mobile, de surplus habituellement monochrome, ce qui est affichable sur un écran de plus grandes dimensions et définition, tel celui d'un micro-ordinateur. Un langage spécifique a été élaboré pour ces usages : le "WML" ("WAP Markup Language"). Il est alors nécessaire de disposer d'un navigateur spécifique.

La plupart des services proposés par les opérateurs de téléphonie ayant recours à la technologie "WAP" concernent des services du type accès aux cotations de bourse, aux prévisions météorologiques, à des horaires de trains

ou autres moyens de transport, aux horaires de spectacles divers, etc., ou à l'affichage de vidéogrammes simples ou à des jeux peu gourmands en ressources informatiques.

Cependant, le recours à cette solution, pour des applications de type commerce électronique ou de type bancaire, par exemple, pose des problèmes relatifs à la sécurité, comme il va l'être montré ci-après.

En effet, un autre besoin qui se fait sentir, dans de nombreux domaines d'application est le niveau de sécurité offert par le système lors des transmissions entre deux entités.

Dans le cadre de l'invention, le terme "sécurité" doit être entendu dans un sens général. Il concerne tout d'abord la confidentialité : certaines données sont dites sensibles et ne doivent pas pouvoir être accessibles, à des entités non autorisées, personnes physiques ou applications logicielles. Pour ce faire, on a recours habituellement à diverses techniques de chiffrage. La sécurité concerne aussi les problèmes d'authentification entre parties, d'autant plus aigus que ces parties peuvent être mobiles sur le réseau Internet. L'authentification peut s'effectuer à l'aide de données d'identification (mots de passe) et/ou en ayant recours à la technique dite de certificats, en association avec des clés de chiffrage, par exemple stockées dans une carte à puce. La sécurité concerne aussi ce qui relève de l'intégrité des données transmises. On doit pouvoir s'assurer que les données reçues n'ont pas subi de modifications non désirées, que ce soit de manière accidentelle (défaillance des circuits de transmission par exemple) ou intentionnelles (malveillance, etc.). Pour ce faire, on peut mettre en œuvre des techniques de redondance et/ou des techniques de signature électronique (scellement).

Pour le réseau Internet "classique", une des techniques de sécurisation les plus utilisées fait appel à la technologie dite "SSL/TLS" ("secure Socket Layer/Transport Layer Security"). Cependant cette technologie n'assure qu'un niveau de sécurité minimal. Un niveau supérieur, d'ailleurs rendu obligatoire par la version dite "IPV6" des protocoles Internet (c'est-à-dire la version 6, la version actuellement utilisée étant majoritairement la version 4 ou "IPV4"), est assuré par le protocole de sécurité connu sous le sigle "IPSec". Il s'agit d'un

niveau de sécurité standardisée permettant une sécurisation de bout en bout, au niveau réseau.

Dans le cas de la technologie "WAP", il a été proposé une couche de sécurité ayant une fonctionnalité analogue à la couche "SSL/TLS" précitée, utilisable pour les transmissions sans fil et connue sous le sigle "WTLS" ("Wireless Transport Layer Security"). Cette technologie, d'usage optionnel, introduit un niveau de complexité important et n'offre pas un niveau de sécurité élevé. Aussi, puisque comme il a été rappelé, la majorité des services offerts ne nécessitant pas de mesures de sécurité particulières, les opérateurs des réseaux téléphoniques sont peu enclin à la mettre en œuvre.

En outre, et surtout, comme il a été indiqué, il existe en général une passerelle, ou "gateway", assurant l'interface entre le réseau Internet et le réseau de transmissions sans fil.

La figure 1, placée en fin de la présente description, illustre schématiquement une architecture, selon l'art connu, d'un système de communication 1 entre un utilisateur U_1 muni d'un terminal mobile de type "WAP" 10 (par exemple un téléphone mobile"), connecté à un réseau de radio-transmission *RTT* (par exemple au standard "GSM" ou "GPRS"), et un dispositif informatique 12, connecté au réseau Internet *RI*, par exemple un serveur éloigné. Le terminal mobile 10 à un rôle de client vis-à-vis du serveur 12. Le réseau *RTT* forme le segment "aérien" du réseau de communication mobile, segment relié à un second segment *RT*, appelé réseau public terrestre mobile, ou sous le sigle anglo-saxon "PLMN" ("Public Land Mobile Networks"), via des balises émettrices/réceptrices (non représentées) définissant des cellules.

Cette technologie est bien connue de l'homme de métier et ne nécessite pas d'être décrite plus avant. On pourra se référer avec profit, à titre d'exemple non limitatif, à l'article de Jean CELLMER, intitulé "Réseaux cellulaires, Système GSM", paru dans les "Techniques de l'Ingénieur", Volume TE 7364, novembre 1999, pages 1 à 23.

Le réseau Internet *RI* est interconnecté au segment *RT*.

Les segments terrestres *RT* et aériens *RTT* sont interconnectés par une passerelle 11. Dans le cadre de la technologie "WAP", cette passerelle 11

joue également un rôle d'interface assurant des conversions bilatérales "WAP" de ou vers "HTTP". Elle comprend notamment une couche logique de protocole "WAP" 110*a* et une couche logique de protocole "HTTP" 111*a*, complétée par une couche de sécurité "SLL/TLS" 111*b*, du côté "HTTP", et une couche (optionnelle) de sécurité "WTLS" 110*b*, du côté "WAP".

La passerelle 11 comprend enfin une interface 113 entre les deux séries de couches logiques destinées à effectuer la conversion bilatérale précitée. Or, précisément, cette interface 113, entre les protocoles de sécurité, "SSL/TLS" 111*b* et "WTSL" 110*b* introduit une faille de sécurité, ce qui crée une zone d'insécurité qui rend le concept dit "WAP gateway" qui vient d'être décrit incompatible, de façon pratique, avec le commerce électronique, les applications bancaires, et de façon plus générale avec toute application dite sensible exigeant un niveau de sécurité élevé.

Par contre, si l'on considère une station de travail 13, ou tout dispositif similaire sous le contrôle d'un usager U_2, connectée directement au réseau Internet *RI*, les protocoles de communication utilisés entre cette station de travail 13 et le serveur 12 restent homogènes. Il n'existe pas de faille de sécurité intrinsèque au système. Il en aurait été de même, si la station de travail 13 avait été connectée au serveur 12 via un réseau intranet ou extranet.

L'invention vise à remplir les besoins qui se font sentir pour les communications via un réseau de type Internet, que ce soit un réseau de type classique ou un réseau mettant en œuvre la technologie "WAP", tout en palliant les inconvénients des dispositifs de l'art connu, et dont certains viennent d'être rappelés.

Pour ce faire, selon une première caractéristique, le concept précité dit "WAP gateway" est entièrement éliminé, ce qui permet de supprimer la faille de sécurité constatée au niveau de l'interface "WEB/WAP". La conversion "WAP/WEB" est effectuée directement au niveau des serveurs.

Selon une deuxième caractéristique, on attribue à chacune des entités devant être mise en relation une adresse dite permanente.

Selon une autre caractéristique, on adopte un mécanisme de sécurité de bout en bout, au niveau réseau, utilisable pour toute application de type

Internet, "WEB", "WAP", ou autre, et qui est programmé de manière déclarative ce qui assure une transparence complète.

Du fait de cette transparence, une des conséquences avantageuses du procédé selon l'invention est qu'il n'est pas nécessaire de réécrire les applications existantes pour les sécuriser avec cette technique.

Dans une variante préférée de réalisation de l'invention, le mécanisme adopté est le protocole "IPSec" précité.

Bien que le procédé selon l'invention soit particulièrement avantageux lorsqu'un des segments du réseau de communication est constitué par un réseau de communication sans fil impliquant l'utilisation de la technologie "WAP", il doit être clair qu'il s'applique également à un réseau de type Internet homogène.

L'invention a donc pour objet principal un procédé de communication sécurisé entre des première et seconde entités interconnectées via un réseau de type Internet, lesdites entités étant associées à des premier et second systèmes de traitement informatique de données parmi un ensemble de systèmes distribués connectés au dit réseau de type Internet, caractérisé en ce que lesdites première et seconde entités sont constituées par une pièce de logicielle hébergée dans un desdits systèmes connectés audit réseau de type Internet et/ou un utilisateur desdits systèmes connectés, en ce que ledit premier système fonctionne en mode dit client et ledit second système fonctionne en mode dit serveur, en ce qu'il comprend une étape d'attribution, sur ledit ensemble de systèmes, d'une adresse permanente de type Internet, du type dit "IP", à chacune desdites entités interconnectées, en ce qu'il est implanté dans ledit second système formant serveur au moins une pièce de logiciel formant serveur et offrant les services d'au moins une application à ladite première entité, et en ce qu'il est implanté dans lesdits premier et second systèmes une pile protocolaire de communication comportant au moins une couche pour l'exécution d'une étape de chiffrement, en mode bout en bout, conforme à un protocole de sécurisation déterminé, de données échangées entre lesdites entités interconnectées.

L'invention a encore pour objet une architecture de communication dans un ensemble de systèmes distribués pour la mise en œuvre du procédé.

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

- la figure 1 illustre schématiquement un exemple de réalisation d'un système de communication, selon l'art connu, comprenant un réseau Internet et un réseau de communication sans fil mettant en œuvre la technologie "WAP" ;
- la figure 2 illustre schématiquement un exemple d'architecture de système de communication via un réseau Internet et un réseau de communication sans fil mettant en œuvre la technologie "WAP", selon un mode de réalisation préféré de l'invention ;
- les figures 3 et 4 illustrent deux variantes de configuration de système serveurs selon l'invention ;
- les figures 5 et 6 illustrent une architecture de système permettant d'adresser directement une application logicielle hébergée par un système ;
- la figure 7 illustre de façon plus détaillée l'interconnexion de deux entités dans le système de la figure 2 ;
- la figure 8 illustre schématiquement une liaison sécurisée du type dit "tunnel" obtenue par le procédé selon l'invention ; et
- la figure 9 illustre un exemple d'architecture de système de communication sécurisée via un réseau Internet pour une application marchande en technologie dite "WAP".

Dans ce qui suit, sans en limiter en quoi que ce soit la portée, on se placera ci-après dans le cadre de l'application préférée de l'invention, sauf mention contraire, c'est-à-dire dans le cas d'un système de communication hybride comprenant un réseau Internet et, éventuellement, un réseau intranet, ainsi qu'un réseau de communication mobile, comportant un segment aérien, et mettant en œuvre la technologie "WAP".

La figure 2 illustre de façon schématique un exemple d'architecture de système, désormais référencée 2, pour la mise en œuvre du procédé conforme

à l'invention. Les éléments communs aux figures précédentes portent les mêmes références et ne seront re-décrits qu'en tant que de besoin.

Le système 2 de l'exemple de la figure 2, considéré dans sa globalité, comprend tout d'abord un terminal mobile 20, sous le contrôle d'un utilisateur U'_1 (jouant un rôle analogue au terminal 10 de la figure 1), et une station mobile 25, sous le contrôle d'un utilisateur U'_3, toutes deux connectées au réseau de radio-transmission *RTT*. Le terminal 20, supposé être un téléphone mobile, est connecté directement au réseau *RTT*. La station mobile 25, par exemple un micro-ordinateur, est connectée à ce réseau *RTT* via un équipement terminal 26, qui peut être constitué également par un téléphone mobile. Ce dernier est connecté à la station mobile 25 via une liaison série ou une liaison infrarouge, par exemple.

Comme précédemment, le réseau *RTT* est connecté au réseau terrestre *RT* par l'intermédiaire d'une passerelle 21. Cependant, cette dernière ne joue plus le rôle d'interface de conversion "WAP – HTTP" (fonction "WAP gateway" précitée), selon un des aspects de l'invention. Elle permet de réaliser, de façon classique en soi, des conversions électriques et logiques nécessaires pour passer d'un mode transmission de données par voie terrestre à un mode de transmission par voie hertzienne, par exemple à la norme "GSM".

Le réseau terrestre *RT* est connecté au réseau Internet *RI*, ce dernier étant, dans l'exemple de la figure 2, connecté lui-même à un réseau intranet *it*, via un serveur d'accès 22. Un serveur 3 est connecté au réseau intranet *it*.

On a également représenté une station de travail 24 connectée au réseau intranet *it*, par exemple un micro-ordinateur, sous le contrôle d'un utilisateur U'_4, ainsi qu'une deuxième station de travail 27 connectée directement au réseau Internet *RI*, par exemple un micro-ordinateur, sous le contrôle d'un utilisateur U'_2 (jouant un rôle analogue à la station 13 de la figure 1).

Dans la réalité, un nombre beaucoup plus importants d'utilisateurs est connecté aux réseaux du système 2, via divers types de machines ou systèmes. Cependant, le système 2 de la figure 2 permet d'illustrer les principaux types de dispositifs rencontrés sur des réseaux où cohabitent les protocoles Internet

standards et "WAP". On peut aussi prévoir des systèmes dits "firewall" ou "pare-feu" (non représentés), par exemple inclus dans le serveur d'accès 22, isolant le réseau intranet *it* du monde extérieur, c'est-à-dire du réseau Internet *RI*.

Selon une caractéristique, également commune en soi à l'art connu, tout ou partie des machines ou systèmes connectés peut être mobile sur le réseau. Les autres utilisateurs devraient pouvoir adresser de façon transparente les machines qui ont migré. Aussi, au moins dans la version "IPV6" précitée, on prévoit un dispositif 23, connu généralement sous la dénomination anglo-saxonne "Home agent", ici connecté au réseau intranet *it*, permettant de gérer cette mobilité. Pour ce faire, un protocole dit "Mobile IP" est utilisé. Il permet de corréler une adresse temporaire attribuée à un système connecté avec une adresse permanente attribuée à l'entité qui lui est associée. Un utilisateur désirant adresser le système mobile ne manipule toujours que cette seule adresse permanente. Le protocole "Mobile IP" précité permet d'organiser une macro-mobilité. C'est le cas, par exemple, lorsque l'on change d'opérateur de réseau "GPRS".

Cet ensemble constitue un système distribué.

Jusqu'à présent, à l'exception de la structure de la passerelle 21, qui ne sert plus d'interface entre les protocoles "WAP/HTTP", l'architecture générale du système 2 qui vient d'être décrite est commune, en soi, à une architecture selon l'art connu (telle celle de la figure 1).

Selon une première caractéristique propre à l'invention, qui va être décrite en regard des figures 3 et 4, l'architecture des serveurs 3 est modifiée, de façon à ce que des conversions aux protocoles d'interfaces applicatives des serveurs "WEB" soient réalisées à l'intérieur de ceux-ci, et non plus au niveau de la passerelle 21, sous la forme de conversion de protocole de communication "WAP/HTTP". Le serveur 3 héberge donc une passerelle "WAP" avec un adaptateur d'interface applicative de serveur "WEB". Cette modification va permettre une sécurisation des transmissions, de bout en bout, transparente vis-à-vis des protocoles utilisés, "HHTP", "WAP" ou autres (transmissions en mode paquet de données), ne présentant plus de faille de sécurité comme dans l'art connu, par la disparition de la fonction "WAP gateway". Elle permet enfin de ne

plus utiliser le protocole de sécurité "WTLS", complexe à mettre en œuvre et n'offrant qu'un faible niveau de sécurité.

Sur la figure 3, on a supposé que le serveur 3 comprenait à la fois des applications "WAP", sous les références 36*a* et 36*b*, et des applications "WEB", sous les références 37*a* et 37*b*. Selon un des aspects de l'invention, on prévoit aussi, implantés dans le serveur 3, un serveur dédié "WAP" 30 et un serveur dédié "WEB" 31. Ces deux serveurs, 30 et 31, sont aptes à reconnaître sélectivement les requêtes selon le protocole "WAP" de celles selon le protocole "WEB", respectivement. Cette sélection s'effectue via les configurations particulières des messages reçus appartenant à l'un ou l'autre des protocoles. Les requêtes sont reçues du réseau Internet *RI*, directement ou indirectement par un réseau intranet *it* (figure 2), via des organes classiques (non représentés) : modem, etc., et des couches de communications standardisées (également non représentées).

Selon une première variante de l'invention, illustrée par la figure 3, on interpose un module 32 entre le serveur "WAP" 30 et des "APIs" ou protocoles d'interface applicatives de type serveur "WEB" 33. Ce module 32, pouvant être constitué par une pièce de logiciel, est un adaptateur d'interface permettant que les méthodes d'accès des applications "WAP" soient les :mêmes que les méthodes d'accès des applications "WEB" à des serveurs "WEB".

Les applications 36*a*-36*b* et 37*a*-37*b* peuvent être constituées de pages écrites en langages "WLM" et "HTLM", respectivement.

Comme il est bien connu en soi, un certain nombre de techniques sont utilisées pour écrire des applications "WEB" en "dos" de serveur "WEB". Il peut s'agir "d'APIs" de types connus sous les sigles "CGI" (pour "Common Gate Interface", qui constituent une passerelle), "NSAPI" (pour Netscape Server API – marque déposée) ou "ISAPI" (pour Internet Server API). L'application 37*b* est de ce type et est donc interconnectée directement au module 33. Plus récemment, on a proposé des "APIs" dits de conteneur (ou "container" selon la terminologie anglo-saxonne) constituant des moteurs dits de "Servlets" (marque déposée). L'application 37*a* est de ce type et est interconnectée au module 33 via un module connu sous l'appellation "WEB Container" 34 et des "APIs"

spécifiques 35. A titre d'exemple, on peut citer "TOMCAT", pour des serveurs de type "APACHE", sous système d'exploitation "LINUX" (tous ces termes correspondant à des marques déposées).

Selon la caractéristique avantageuse de l'invention qui vient d'être rappelée, le serveur "WAP" 30 dispose donc d'un adaptateur d'interface 32 qui permet aux applications écrites pour des serveurs "WAP" 30 d'utiliser les deux séries de mécanismes standards rappelés ci-dessus : applications "WAP" 36*b* et 36*a* respectivement.

Une deuxième variante de réalisation de l'invention est illustrée par la figure 4. Le serveur, ici référencé 3', comprend, comme précédemment, un serveur "WAP" 30 et un serveur "WEB" 31, ainsi que le module adaptateur d'interface 32. Cependant les applications présentes dans le serveur 3' sont uniquement des applications de type "WEB", référencées 37*a* à 37*d*, *a priori* écrites en langage "HTLM". Les applications "WEB" 37*a* et 37*b* correspondent aux applications "WEB" de mêmes références sur la figure 3, les applications 37*c* et 37*d* se substituant aux applications "WAP" 36*a* et 36*b*, respectivement. Des modules supplémentaires 38*a* et 38*b* sont intercalés entre les modules 33 et 34-35, d'une part, et les applications 38*a* et 38*b*, d'autre part. La fonction dévolue à ces module 38*a* et 38*b* est une conversion bidirectionnelle entre les langages "HTML" et "WML". De ce fait, les requêtes en provenance du serveur "WAP" 30 sont transmises via les modules 33 ou 34-35 aux convertisseurs 38*a* ou 38*b*, puis à une des applications "WEB" 37*c* ou 37*d*. Par contre, les requêtes en provenance du serveur "WEB" 31 sont transmises directement, des modules 33 ou 34-35 aux applications "WEB" 37*a* ou 37*b*. Le cheminement inverse est également vrai.

Selon une autre caractéristique du procédé de l'invention, une adresse permanente est attribuée aux utilisateurs ou à des applications clientes (par exemple U_1 à U_4, figure 2), et aux applications serveurs (par exemple 36*a*-36*b* et/ou 37*a*-37*b*, figures 3 ou 4). De façon générale, on attribue une adresse permanente aux entités devant être connectées. Cette attribution peut être effectuée de façon dynamique.

Dans les réseaux de type Internet actuels, il n'est pas possible d'adresser directement une application à l'intérieur d'un système. En général, des clients qui adressent une entité distante gérée par un système, service ou application, invoquent un service de noms. Celui-ci requiert le nom du réseau et l'adresse du système qui contient l'entité à atteindre.

Aussi, la Demanderesse a proposé, dans la demande de brevet français publiée sous le numéro FR 2 773 428 A1, un procédé permettant notamment d'adresser directement une application logicielle hébergée par un système connecté à un réseau de type Internet. Ce procédé va être rappelé brièvement ci-après par référence aux figures 5 et 6.

Cette figure 5 illustre schématiquement le procédé d'adressage de serveurs selon cette demande de brevet. Pour simplifier, il a été supposé que l'ensemble des systèmes, référencé 2', était compris dans un domaine D_1 unique, associé à un serveur de noms de domaine DNS_1. On a représenté, également dans un but de simplification, un seul client, CI_1. Il peut s'agir, par exemple, de la station de travail 27 de la figure 2. Selon une des caractéristiques du procédé d'adressage, chaque système réel (par exemple les serveurs 3 ou 3' des figures 3 et 4) est assimilé à un réseau virtuel, référencés SVN_1 à SVN_n, représentés en traits pointillés sur la figure 5, appelés arbitrairement "réseaux virtuels systèmes".

Selon une deuxième caractéristique du procédé d'adressage, les serveurs, par exemple SV_{11} à SV_{13} dans le réseau virtuel système SVN_1, sont associés chacun à une adresse "IP" individuelle. Il s'ensuit que chaque serveur, par exemple le serveur SV_{11}, c'est-à-dire un objet ou une entité logicielle, est directement adressable par un client, par exemple le client CI_1, et, de façon plus générale, un client CI_x, si le système 2' comporte plusieurs clients (x étant arbitraire). En d'autres termes, un client n'a plus besoin de connaître le nom du système hébergeant le serveur recherché. L'annuaire du serveur DNS_1 stocke toutes les adresses "IP" des serveurs, par exemple des serveurs SV_{11} à SV_{13} du réseau virtuel système SVN_1.

Il doit être noté que, dans un système multidomaines, tous les serveurs d'un réseau virtuel système appartiennent à un même domaine.

Selon une troisième caractéristique du procédé d'adressage, les systèmes "réels" ou machines qui constituent, dans une configuration classique, des systèmes terminaux deviennent des systèmes intermédiaires. Ils constituent des nœuds des réseaux virtuels, SVN_1 à SVN_n, et également des nœuds du réseau "réel", c'est-à-dire le sous-réseau Internet ou intranet SR_X. Les systèmes agissent en tant que passerelles qui interconnectent les nœuds des réseaux virtuels, SVN_1 à SVN_n, au sous-réseau SR_X. Chaque système est également doté d'une adresse "IP".

On peut donc représenter un réseau virtuel système SVN_1 associé à un système S_1 de la façon illustrée par la figure 6. On constate qu'un système S_1 constitue bien un nœud pour le réseau R_X et qu'il est associé, vu de ce réseau (c'est-à-dire de l'extérieur), à une première adresse IP_1, avec $@IP_1{:}X,X_1$, X étant le préfixe attribué au sous-réseau SR_X et X_1 l'adresse de S_1 dans le sous-réseau SR_X.

On suppose que le réseau virtuel système SVN_y est constitué des deux serveurs référencés SV_A et SV_B qu'il héberge et du système S_1 proprement dit. Vu du réseau virtuel système SVN_1, le système S_1 est associé à une seconde adresse : IP_2, avec @ $IP_2{:}Y,Y_1$, Y étant le préfixe attribué au réseau virtuel système SVN_y et Y_1 l'adresse de S_1 dans le réseau SVN_y.

De même, les serveurs SV_A et SV_B sont associés à deux adresses, IP_A et IP_B, respectivement, avec @ $IP_A{:}Y,Y_A$, et @ $IP_B{:}Y,Y_B$, Y_A et Y_B étant les adresses de SV_A et SV_B, respectivement, dans le réseau SVN_y.

Pour une description plus détaillée du mécanisme d'adressage, on pourra se référer avec profit à la demande de brevet français précitée, notamment à la figure 4 de cette demande qui illustre de façon détaillée l'architecture d'un système réel permettant l'adressage précité.

Dans le cadre de l'invention, les serveurs SV_A et SV_B peuvent être constitués par les serveurs "WAP" 30 et "WEB" 31 de la figure 3, le système réel S_1 étant alors le système serveur 3.

Le procédé d'adressage selon la demande de brevet français précité, comme le procédé selon l'invention restent compatibles avec le protocole Internet le plus couramment utilisé ce jour, c'est-à-dire la version "IPV4".

Cependant, une adresse conforme à ce protocole ne comporte que quatre octets, soit 2^{32} adresses théoriques, en réalité beaucoup moins du fait de la structure hiérarchique rappelée ci-dessus. Du fait de la croissance rapide du réseau Internet, des projections sur le futur ont montré que cet espace d'adressage limité conduira rapidement à une pénurie. Or le fait de pouvoir adresser directement des entités internes à un système et, selon une des caractéristiques de l'invention, de leur attribuer des adresses permanentes, multiplie les besoins en nombres d'adresses distinctes. Aussi, dans le cadre de l'invention, on préférera le protocole "IPV6" pour l'attribution des adresses permanentes. L'espace d'adressage théorique est alors fortement augmenté : environ $6{,}65\times10^{23}$ adresses réseau par mètre carré de la surface de la terre.

Comme il a été indiqué, selon une autre caractéristique de l'invention, la sécurisation des transmissions est réalisée de bout en bout, de façon transparente par vis-à-vis des différents protocoles : "WAP", "WEB" ou autres. Dans un mode de réalisation préféré, on adopte le protocole connu sous le sigle "IPSec", protocole d'ailleurs obligatoire si la version "IPV6" est mise en œuvre pour les transmissions sur le réseau Internet.

La figure 7 illustre schématiquement un exemple d'architecture de système de transmission 2, selon l'invention, montrant l'interconnexion entre deux entités de type client, référencées 4 et 4', et une entité de type serveur, 3. Les client 4 ou 4' est constitués par l'un des dispositifs représentés sur la figure 2 : 20, 24, 26 ou 27. Les deux entités, 3 et 4 ou 4', communiquent entre elles par l'intermédiaire d'un ou plusieurs des réseaux de la figure 2, sous la référence unique *R*. L'entité 4 est un client de type "WEB" et l'entité 4' un client de type "WAP".

On a supposé que le protocole "IPV4" était utilisé pour les transmissions, ce qui est généralement le cas à l'heure actuelle. Le procédé d'adressage illustré par référence avec les figures 5 et 6, et le procédé selon l'invention sont compatibles avec des réseaux de type, comme il a été rappelé. Dans le cadre de l'invention, on met en œuvre un protocole dénommé "6-to-4" qui convertit les adresses "IPV6" en adresses "IPV4" compatibles "IPV6", et inversement.

Selon le procédé de l'invention on implémente dans chaque système physique une pile protocolaire de communication comprenant successivement une pile "IPV6", 390 ou 44, incluant le protocole de sécurité "IPSec", 391 ou 45, et une pile "IPV4" 392 ou 46, respectivement pour le serveur 3 et les clients 4 ou 4'. Les piles "IPV4", 392 et 46, sont interfacées avec le réseau *R*. Les piles "IPV6", 390 et 44, sont interfacées avec les serveurs "WAP" 30 et "WEB" 31, côté serveur 3, et avec des clients "WAP" 42 et "WEB" 43, côté client 4.

Sur la figure 7, on a également détaillé les couches applicatives du client 4, qui présentent une grande symétrie avec celles du serveur 3. les clients, 42 et 42', peuvent être constitués par des navigateurs. Des associations de sécurité sont définies entre des utilisateurs ou des applications clientes et des applications serveurs. De façon avantageuse, un "triplet" identifie chaque association de sécurité :

- une adresse de destination des paquets de données ;
- un protocole de sécurité, de façon préférentielle le protocole dit "ESP" ("Encapsulating Security Payload" ou protocole d'authentification de données) est utilisé en mode tunnel ; et
- un paramètre index de sécurité ("Security Parameter Index" ou "SPI").

On constate que la sécurisation des transmissions, du fait que le chiffrage et le déchiffrage est réalisé en amont des couches d'adresses "IPV4", dans chaque entité à mettre en relation, on obtient bien la sécurisation transparente désirée, de bout en bout. On ne constate plus de faille de sécurité lors du cheminement des données, même si un segment du réseau est du type à transmissions sans fil.

Le schéma équivalent à l'architecture représentée par la figure 7 est celui illustré par la figure 8. Le canal de transmission peut en effet être représenté symboliquement sous la forme d'un câble blindé ou "tunnel" mettant en liaison deux entités, arbitrairement référencées E_1 et E_2, auxquelles les adresses permanentes respectives $@IP_{E1}$ et $@IP_{E2}$ ont été attribuées. Il s'agit, soit d'adresses "IPV6", soit d'adresses compatibles "IPV6" si le réseau est au protocole ""IPV4".

A titre d'exemple, un "tunnel" sécurisé est établi entre un terminal "WAP", par exemple le téléphone mobile 20 (figure 2) et le serveur 3 hébergeant une application "WAP" 33. De façon générale, le "tunnel" transporte des communications "IPV6" de bout en bout entre un utilisateur et une application.

Naturellement, si le réseau *R* est au protocole "IPV6" les conversions d'adresses ne sont plus nécessaires et les piles "IPV4", 392 et 46 n'existent pas.

Lorsque la station connectée est du type mobile, on fait appel au protocole dit "mobile IPV6". La station mobile est associée à chaque instant à une adresse temporaire qui reste transparente pour les utilisateurs désirant adresser l'entité associée à cette station. Un dialogue est initialisé avec un dispositif du type "home agent" précité (figure 2 : 23). Ce dernier établit une corrélation entre l'adresse permanente attribuée et l'adresse temporaire. Cette disposition permet d'obtenir ce qui a été précédemment appelée une "macro-mobilité".

Le dialogue précité est sécurisé. De façon préférentielle, le mécanisme d'authentification propre à "IPSec" est mis en œuvre comme le préconise le protocole "mobile IPV6".

On obtient des communications entre utilisateurs et applications avec mise en œuvre des services suivants de "IPSec", s'ils sont sélectionnés :

- authentification de la source de données, incluant l'authentification de l'utilisateur ;
- intégrité ; et
- confidentialité.

En ce qui concerne plus précisément l'authentification des utilisateurs, celle-ci s'effectue avantageusement par l'intermédiaire de l'adresse permanente qui leur est attribuée. Les utilisateurs sont enregistrés dans un annuaire électronique. A titre d'exemple, l'organisme connu sous le sigle "IETF" ("Internet Engineering Task Force") a proposé un standard d'annuaire, que l'on peut qualifier d' "allégé", connu sous le sigle "LDAP" ("Lightweight Directory Access Protocol"). Un profil d'abonné et des privilèges éventuels sont associés à l'utilisateur. Comme "IPSec" est utilisé, avec le mécanisme "ESP", en mode

"tunnel" (figure 8), une authentification de la source d'information (une adresse "IPV6" permanente), en l'occurrence l'identification de l'utilisateur, est présente dans chaque paquet de données et chiffrée. En outre, la source de données est authentifiée et, dans ce cas, représente l'utilisateur. Cette identification est utilisée pour construire un contexte de sécurité utilisé lui-même par l'application ou, mieux, par le contenant de l'application pour effectuer un contrôle d'accès pour des contrôles d'autorisation.

Pour fixer les idées, on va maintenant décrire un exemple d'architecture de système de transmission, mettant en œuvre les dispositions de l'invention, adaptée à une application marchande mobile sécurisée, empruntant un tronçon de réseau de radio-transmission par paquets, par exemple du type "GPRS".

La figure 9 illustre schématiquement une telle architecture, référencée 2". Les éléments communs aux figures précédentes portent les mêmes références et ne seront re-décrits qu'en tant que de besoin.

Comme précédemment, le système 2", dans sa globalité comprend des terminaux mobiles, dont un seul, 20 sous le contrôle de l'utilisateur U_1, a été illustré. Ce terminal mobile 20 est connecté au tronçon de réseau sans fil *RTT*, puis via la passerelle 21 au réseau terrestre public *RT*, au réseau Internet *RI*. Un serveur, par exemple du type 3 de la figure 3, hébergeant au moins une application marchande par exemple l'application 36*a*, en technologie "WAP", est connecté au réseau Internet via le réseau Intranet *it* et le serveur d'accès 22. On a également représenté un terminal "WEB" 24 connecté au réseau intranet *it*. Ce terminal est similaire à la station 24 de la figure 2.

On n'a pas représenté les piles protocolaires d'adressage et "IPSec" (voir figure 7) permettant d'attribuer des adresses "IPV6" et d'effectuer les opérations nécessitées par le protocole "IPSec".

L'architecture qui vient d'être décrite permet d'établir un lien logique *lls* entre l'utilisateur U_1 et l'application marchande "WAP" 36*a*, sécurisé de bout en bout, ce malgré le fait qu'il emprunte un segment de réseau sans fil.

A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 2 à 9.

Les applications de l'invention ne se limitent pas non plus au seul domaine "commerce électronique sécurisé". Elles couvrent également des applications bancaires, médicales, et de façon plus générale toute application mettant en œuvre des communications transitant par un réseau de type Internet, notamment dont un segment au moins est constitué par un réseau de transmissions sans fil.

REVENDICATIONS

1. Procédé de communication sécurisé entre des première et seconde entités interconnectées via un réseau de type Internet, lesdites entités étant associées à des premier et second systèmes de traitement informatique de données parmi un ensemble de systèmes distribués connectés au dit réseau de type Internet, caractérisé en ce que lesdites première et seconde entités sont constituées par une pièce de logicielle (36*a*-36*b*, 37*a*-37*b*) hébergée dans un desdits systèmes (3, 3') connectés audit réseau de type Internet (*RI*, *R*) et/ou un utilisateur (U_1) desdits systèmes connectés (4, 20), en ce que ledit premier système (4, 20) fonctionne en mode dit client et ledit second système (3, 3') fonctionne en mode dit serveur, en ce qu'il comprend une étape d'attribution, sur ledit ensemble de systèmes, d'une adresse permanente de type Internet, du type dit "IP", à chacune desdites entités interconnectées (U_1, 36*a*-36*b*, 37*a*-37*d*), en ce qu'il est implanté dans ledit second système formant serveur (3, 3') au moins une pièce de logiciel formant serveur (30, 31) et offrant les services d'au moins une application (36*a*-36*b*, 37*a*-37*d*) à ladite première entité (U_1), et en ce qu'il est implanté dans lesdits premier (4, 20) et second (3, 3') systèmes une pile protocolaire de communication comportant au moins une couche (45, 391) pour l'exécution d'une étape de chiffrement, en mode bout en bout, conforme à un protocole de sécurisation déterminé, de données échangées entre lesdites entités interconnectées (U_1, 36*a*-36*b*, 37*a*-37*d*).

2. Procédé selon la revendication 1, caractérisé en ce que lesdites adresses permanentes "IP" attribuées aux dites entités interconnectées (U_1, 36*a*-36*b*, 37*a*-37*d*) sont conformes au protocole d'adressage de type Internet "IPV6".

3. Procédé selon la revendication 2, caractérisé en ce que lesdites communications sur ledit réseau de type Internet (*RI*, *R*) s'effectuant selon le protocole d'adressage de type Internet "IPV4", il comprend l'implantation dans lesdits premier (4, 20) et second (3, 3') systèmes d'une couche protocolaire

(46, 392) permettant de dériver des adresses "IPV4", compatibles avec ledit protocole "IPV6", par l'exécution d'une étape de conversion d'adresses conforme au protocole dit "6-to-4".

4. Procédé selon la revendication 1, caractérisé en ce que ladite étape de chiffrement est effectuée conformément au protocole dit "IPSec", utilisé avec le mécanisme dit "EPS" d'authentification de sources d'information, en mode dit "tunnel", de manière à obtenir des échanges de données sécurisées entre lesdites entités interconnectées (U_1, 36*a*-36*b*, 37*a*-37*d*).

5. Procédé selon la revendication 4, caractérisé en ce que, ladite première entité étant un utilisateur (U_1) dudit premier système (4, 20), il comprend une étape d'authentification dudit utilisateur (U_1) et en ce que ladite adresse "IP" est utilisée comme donnée d'identification de cet utilisateur (U_1).

6. Procédé selon la revendication 5, caractérisé en ce que lesdites communications s'effectuant en mode paquets de données, lesdites données d'identification d'utilisateur (U_1) sont présentes, sous forme chiffrée conforme au dit protocole "IPSec", dans chacun desdits paquets de données.

7. Procédé selon la revendication 1, caractérisé en ce que ledit premier système (4, 20) est connecté à un segment de transmissions sans fil (*RTT*), en ce que les communications entre ce premier système constituant un système client (4, 20) et ledit second système constituant un système serveur (3, 3') s'effectuent selon le protocole dit "WAP", et en ce qu'il comprend l'implantation dans ledit second système (3, 3') d'au moins une pièce de logiciel constituant un serveur "WAP" (30) et un deuxième pièce de logiciel (32) formant une interface unifiée entre ledit serveur "WAP" (30) et au moins une application (36*a*-36*b*, 37*a*-37*d*) offrant ses services à ladite première entité (U_1), de manière à ce que ledit serveur "WAP" (30) soit intégré en tant que serveur "WEB" dans ledit système serveur (3, 3').

8. Procédé selon la revendication 7, caractérisé en ce qu'il comprend l'implantation dans ledit second système (3, 3') d'un module supplémentaire

(35) d'adaptation bilatérale d'interface de structures permettant de supporter des interfaces applicatives (33) utilisées par les serveurs de type "WEB".

9. Procédé selon la revendication 7, caractérisé en ce qu'il comprend l'implantation dans ledit premier système (4, 20) d'une pièce de logiciel constituant un client et en ce que cette pièce de logiciel est un navigateur de type "WAP".

10. Procédé selon la revendication 1, caractérisé en ce que ledit premier système étant un système mobile (25), il comprend l'attribution au dit premier système (25) d'une adresse temporaire, en ce qu'il comprend une étape de dialogue entre ledit premier système (25) et un organe d'un type dit "home agent" (23), connecté au dit réseau de type Internet (*it*), permettant de corréler à chaque instant ladite adresse permanente, attribuée à ladite première entité (U'_3), avec ladite adresse temporaire, selon un protocole dit "mobile IPV6 protocol".

11. Architecture de système de communication sécurisé entre des première et seconde entités interconnectées via un réseau de type Internet, lesdites entités étant associées à des premier et second systèmes de traitement informatique de données parmi un ensemble de systèmes distribués connectés au dit réseau de type Internet, caractérisée en ce que le dit premier système (4, 20) est un système fonctionnant en mode dit client et ledit second système (3, 3') un système fonctionnant en mode dit serveur, en ce que lesdites première et seconde entités sont des pièces de logicielles (36*a*-36*b*, 37*a*-37*d*) hébergées dans lesdits premier (4, 20) et second (3, 3') systèmes et/ou un utilisateur (U_1) desdits systèmes connectés, en ce lesdites entités (U_1, 36*a*-36*b*, 37*a*-37*d*) sont associées à des adresses permanentes de type Internet, du type dit "IP", en ce que ledit second système (3, 3') formant serveur comprend au moins une pièce de logiciel (31) formant serveur (30, 31) et offrant les services d'au moins une application (36*a*-36*b*, 37*a*-37*d*) à ladite première entité (U_1), et en ce que lesdits premier (4, 20) et second (3, 3') systèmes comprennent une pile protocolaire de communication

comportant au moins une couche d'adressage (44, 390) selon ladite adresse "IP" permanente et une couche logique (45, 391) pour l'exécution d'une étape de chiffrement, en mode bout en bout, conforme à un protocole de sécurisation déterminé, de données échangées entre lesdites entités interconnectées (U_1, 36*a*-36*b*, 37*a*-37*d*).

12. Architecture selon la revendication 11, caractérisée en ce que ladite couche d'adressage (44, 390) est conforme au protocole "IPV6".

13. Architecture selon la revendication 12, caractérisée en ce que ledit réseau de type Internet (*R*) véhiculant des paquets de données conforme au protocole "IPV4", lesdites piles protocolaires desdits premier (4, 20) et second (3, 3') systèmes comprennent chacune une première couche d'adressage (44, 390) selon ladite adresse "IP" au protocole "IPV6" et une seconde couche (46, 392) d'adressage au protocole "IPV4" dont vont être dérivées des adresses compatibles "IPV6" de manière à obtenir des échanges en mode dit "tunnel" ; lesdites couches logiques (45, 391) exécutant une étape de chiffrement (45, 37) en faveur desdits paquets de données échangés entre lesdites entités interconnectées (U_1, 36*a*-36*b*, 37*a*-37*d*).

14. Architecture selon la revendication 11, caractérisée en ce que lesdites couches logiques (45, 391) pour l'exécution d'une étape de chiffrement sont conformes au protocole dit "IPSec", utilisé avec le mécanisme dit "EPS" d'identification de sources d'information, en mode dit "tunnel", de manière à obtenir des échanges de données sécurisées entre lesdites entités interconnectées (U_1, 36*a*-36*b*, 37*a*-37*d*),

15. Architecture selon la revendication 11, caractérisée en ce que ledit premier système (4, 20) est connecté à un segment de transmissions sans fil (*RTT*), en ce que les communications entre ce premier système (4, 20), constituant un système client, et ledit second système (3, 3'), constituant un système serveur, s'effectuent selon le protocole dit "WAP", et en ce que ledit second système (3, 3') comprend au moins un premier module constituant un serveur

"WAP" (30) et un deuxième module (32) formant une interface unifiée entre ledit serveur "WAP" (30) et au moins une application (36*a*-36*b*, 37*a*-37*d*) offrant ses services à ladite première entité (U_1), de manière à ce que ledit serveur "WAP" (30) soit intégré en tant que serveur "WEB" dans ledit système serveur (3, 3').

16. Architecture selon la revendication 15, caractérisée en ce que ledit second système (3, 3') comprend au moins un module supplémentaire (38*a*-38*b*) de conversion bilatérale de paquets de données de structures conformes aux dits protocoles "WEB" ou "WAP".

17. Architecture selon la revendication 15, caractérisé en ce que ledit premier système est un terminal de téléphonie mobile (20, 4) à la norme dite "GSM", en ce qu'il comprend un navigateur de type WAP constituant un client, et en ce qu'il comprend un écran de visualisation pour l'affichage de pages en langage du type dit "WML".

18. Architecture selon la revendication 15, caractérisé en ce que ledit premier système est un terminal de téléphonie mobile à la norme dite "GPRS" et en ce qu'il comprend un navigateur de type Internet constituant un client, et en ce qu'il comprend un écran de visualisation pour l'affichage de pages en langage du type dit "WML".

ABREGE

Procédé et architecture de système de communication sécurisé entre deux entités connectées à un réseau de type Internet comprenant un segment de transmissions sans fil

L'invention concerne un procédé et une architecture de communication sécurisée entre deux entités (U_1, 36*a*) associées à un système (10, 3') et interconnectées à un réseau Internet (*RI*, *R*) comprenant un segment de transmissions sans fil (*RTT*). Les entités sont des applications logicielles (36*a*) hébergées par les systèmes (3') et/ou des utilisateurs (U_1) de ces systèmes (10). L'un des systèmes est un terminal (10) en technologie "WAP" connecté au segment de transmissions sans fil (*RTT*), constituant un système client, l'autre un système serveur (3'). Une adresse permanente réseau est attribuée aux deux entités (U_1, 36*a*), de façon préférentielle conforme au protocole "IPV6". Les systèmes serveur (3') et client (10) comprennent une pile protocolaire de communication comprenant des niveaux d'adressage "IP" et de sécurisation de bout en bout, de façon préférentielle conformément au protocole "IPSec" qui assure des services d'authentification de confidentialité et d'intégrité. Le système serveur (3') comprend couche logique supplémentaire (32) permettant à un serveur "WAP " intégré, de disposer d'interfaces applicatives identiques à celles utilisées communément par les serveurs "WEB".

FIGURE 9

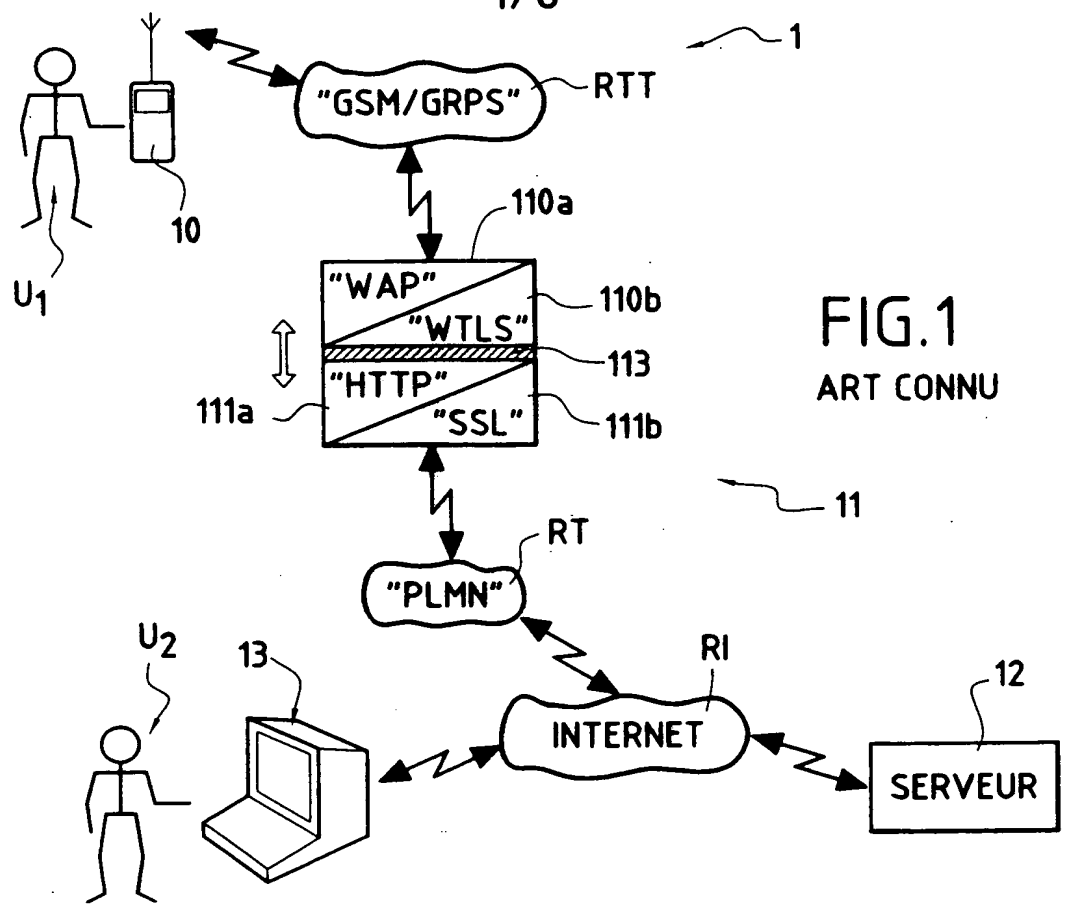


FIG.1
ART CONNU

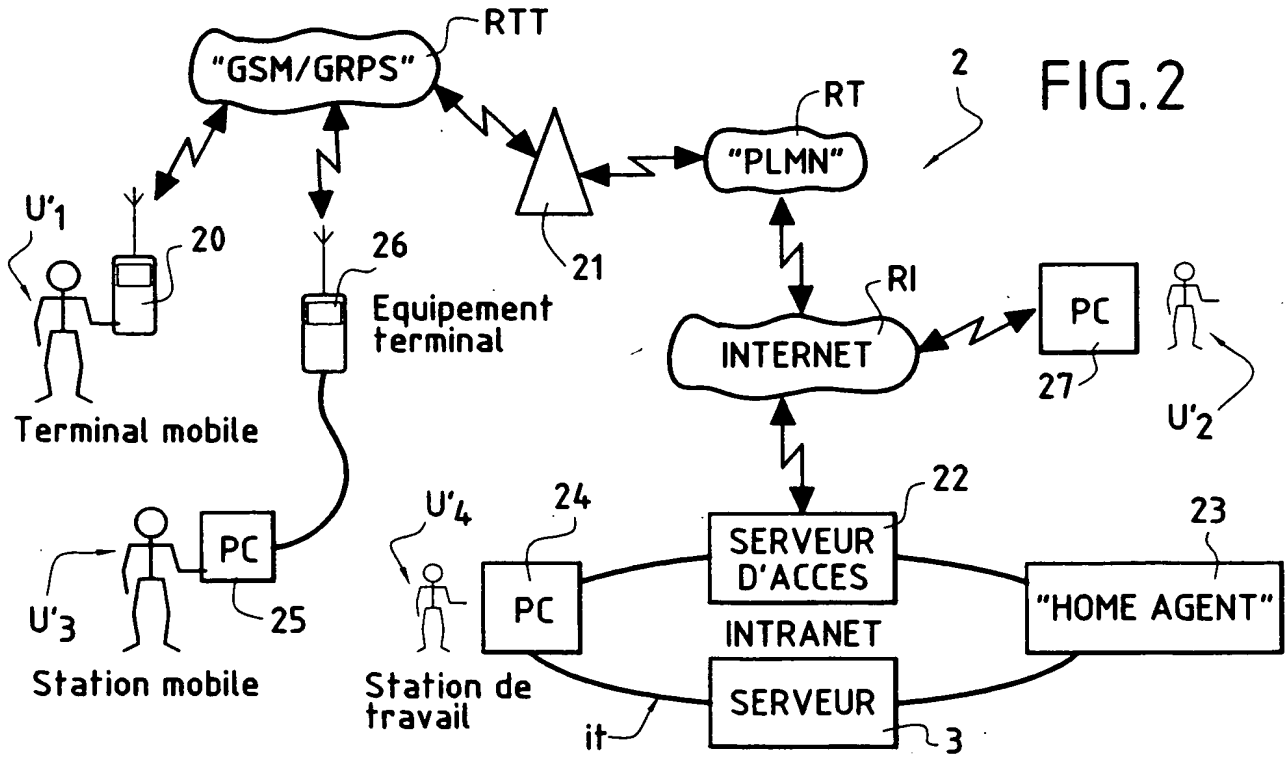


FIG.2

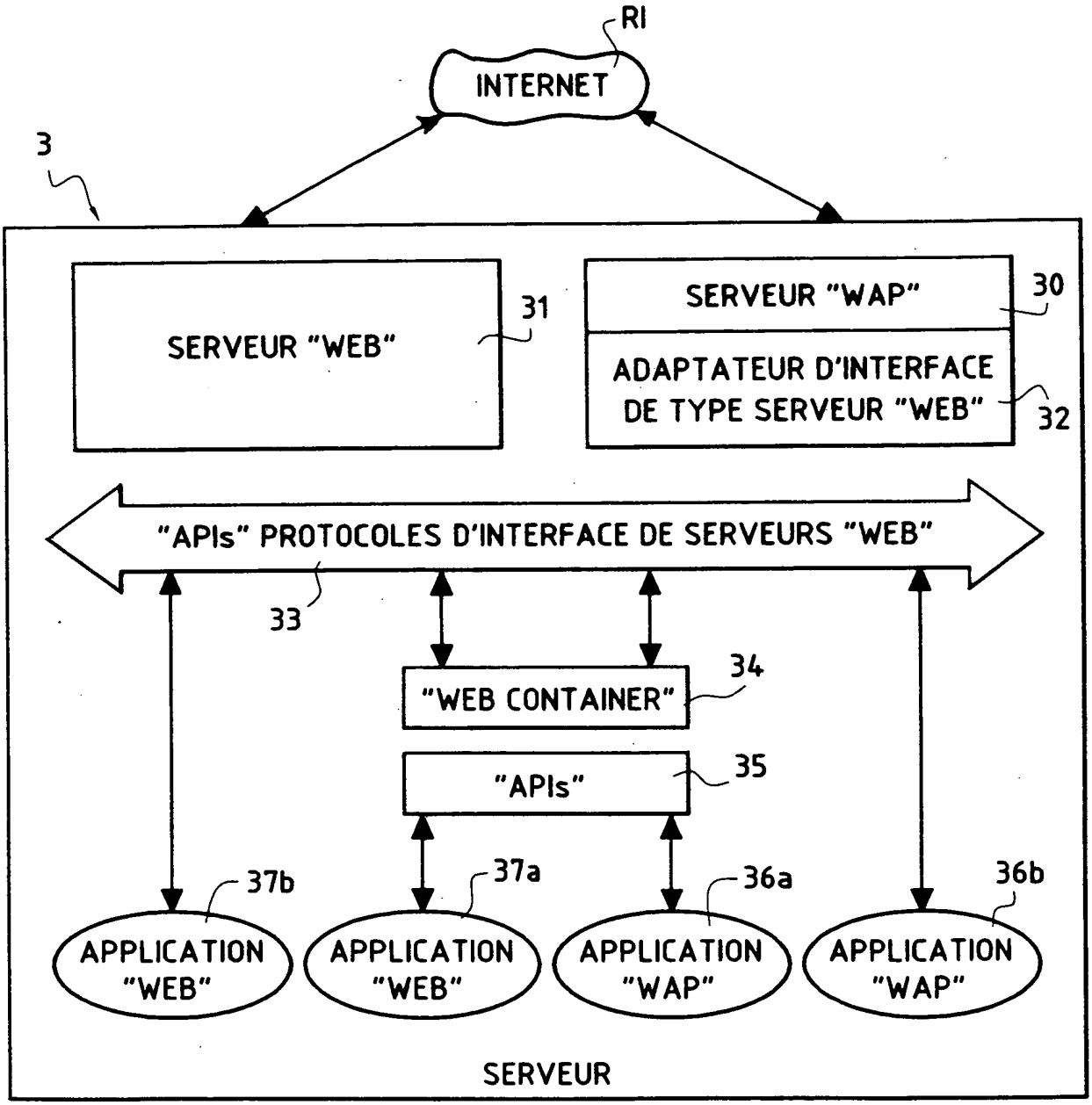

RI
INTERNET
3
SERVEUR "WEB"
31
SERVEUR "WAP"
30
ADAPTATEUR D'INTERFACE DE TYPE SERVEUR "WEB"
32
"APIs" PROTOCOLES D'INTERFACE DE SERVEURS "WEB"
33
"WEB CONTAINER"
34
"APIs"
35
37b
37a
36a
36b
APPLICATION "WEB"
APPLICATION "WEB"
APPLICATION "WAP"
APPLICATION "WAP"
SERVEUR

FIG.3

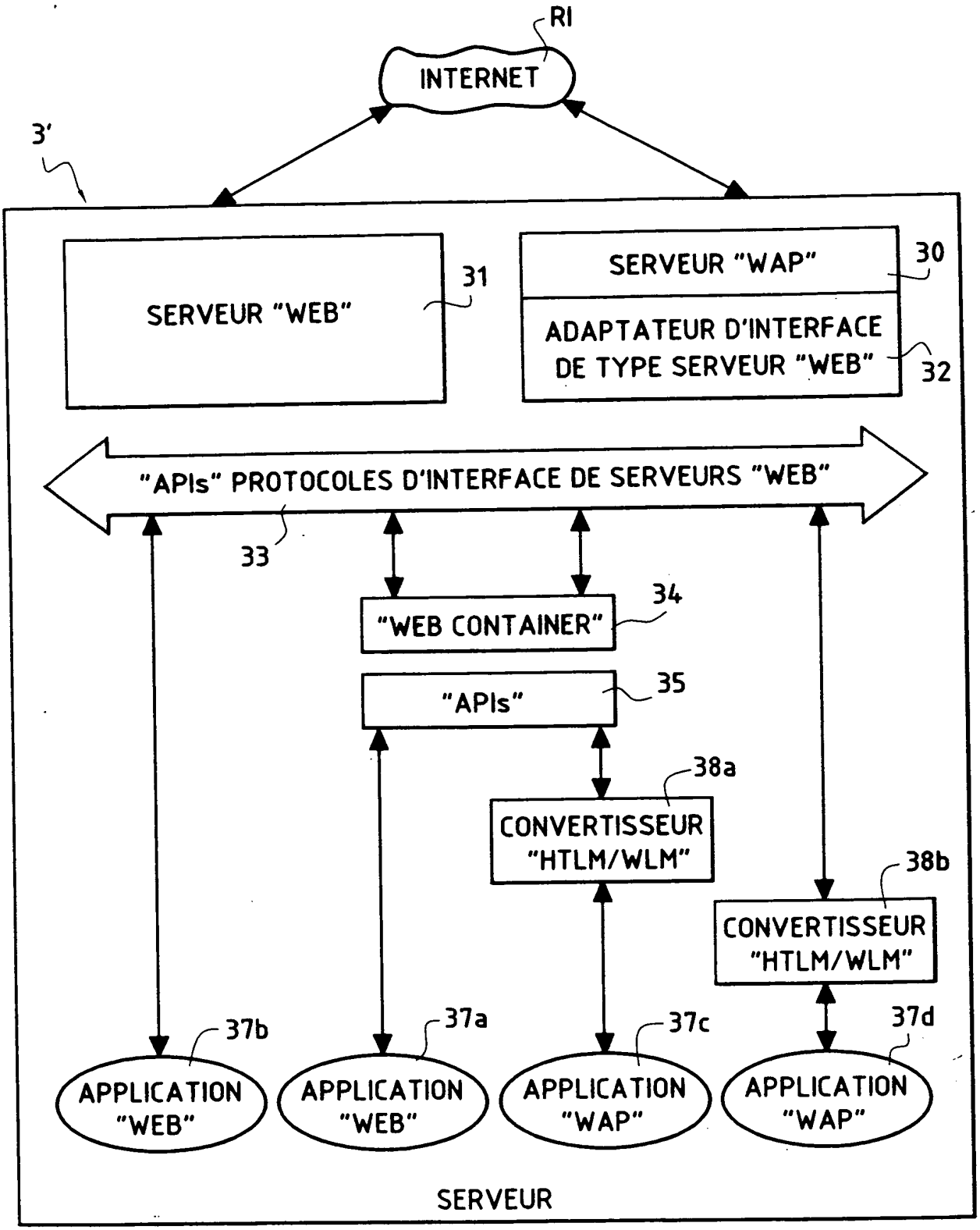
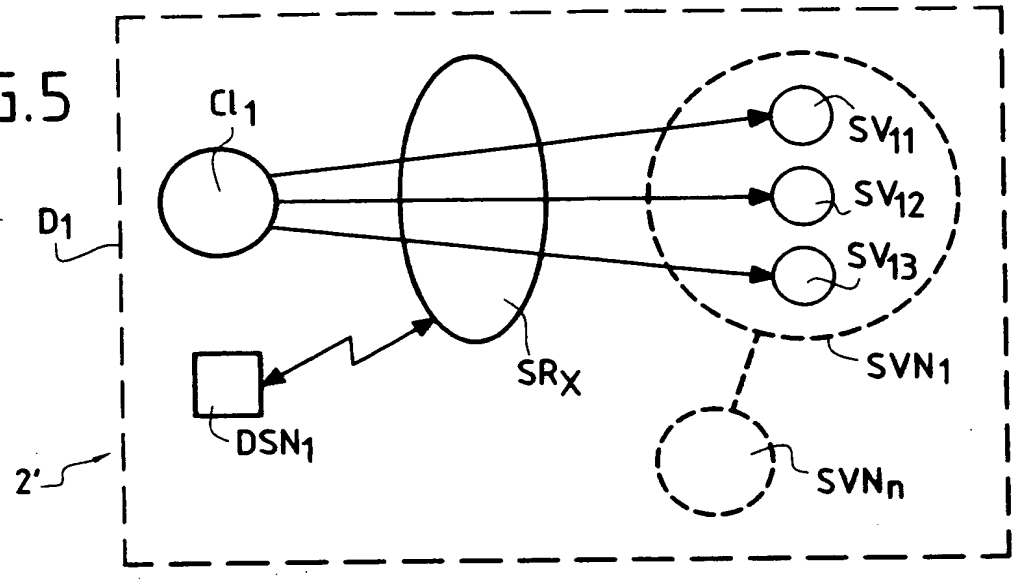

RI
INTERNET
3'
SERVEUR "WEB"
31
SERVEUR "WAP"
30
ADAPTATEUR D'INTERFACE DE TYPE SERVEUR "WEB"
32
"APIs" PROTOCOLES D'INTERFACE DE SERVEURS "WEB"
33
"WEB CONTAINER"
34
"APIs"
35
38a
CONVERTISSEUR "HTLM/WLM"
38b
CONVERTISSEUR "HTLM/WLM"
37b
37a
37c
37d
APPLICATION "WEB"
APPLICATION "WEB"
APPLICATION "WAP"
APPLICATION "WAP"
SERVEUR

FIG.4

FIG.5



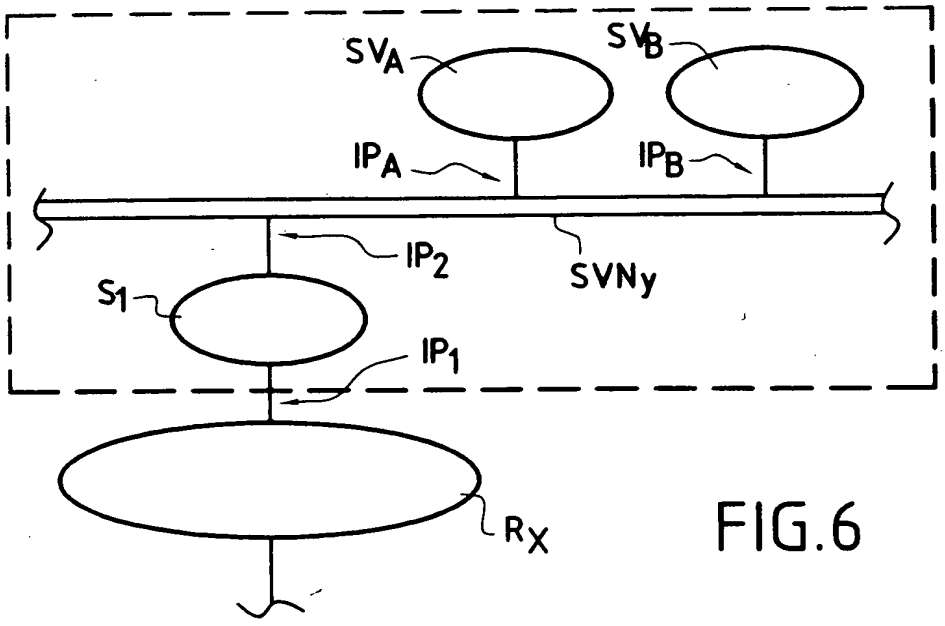


FIG.6

FIG.8

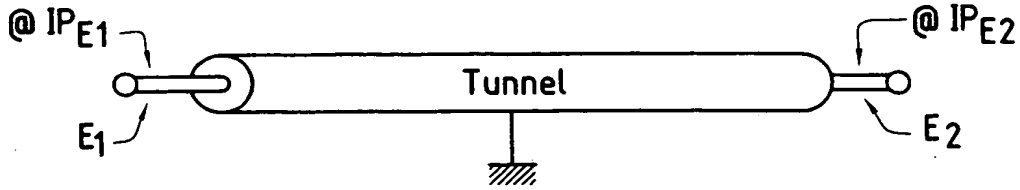


FIG.7

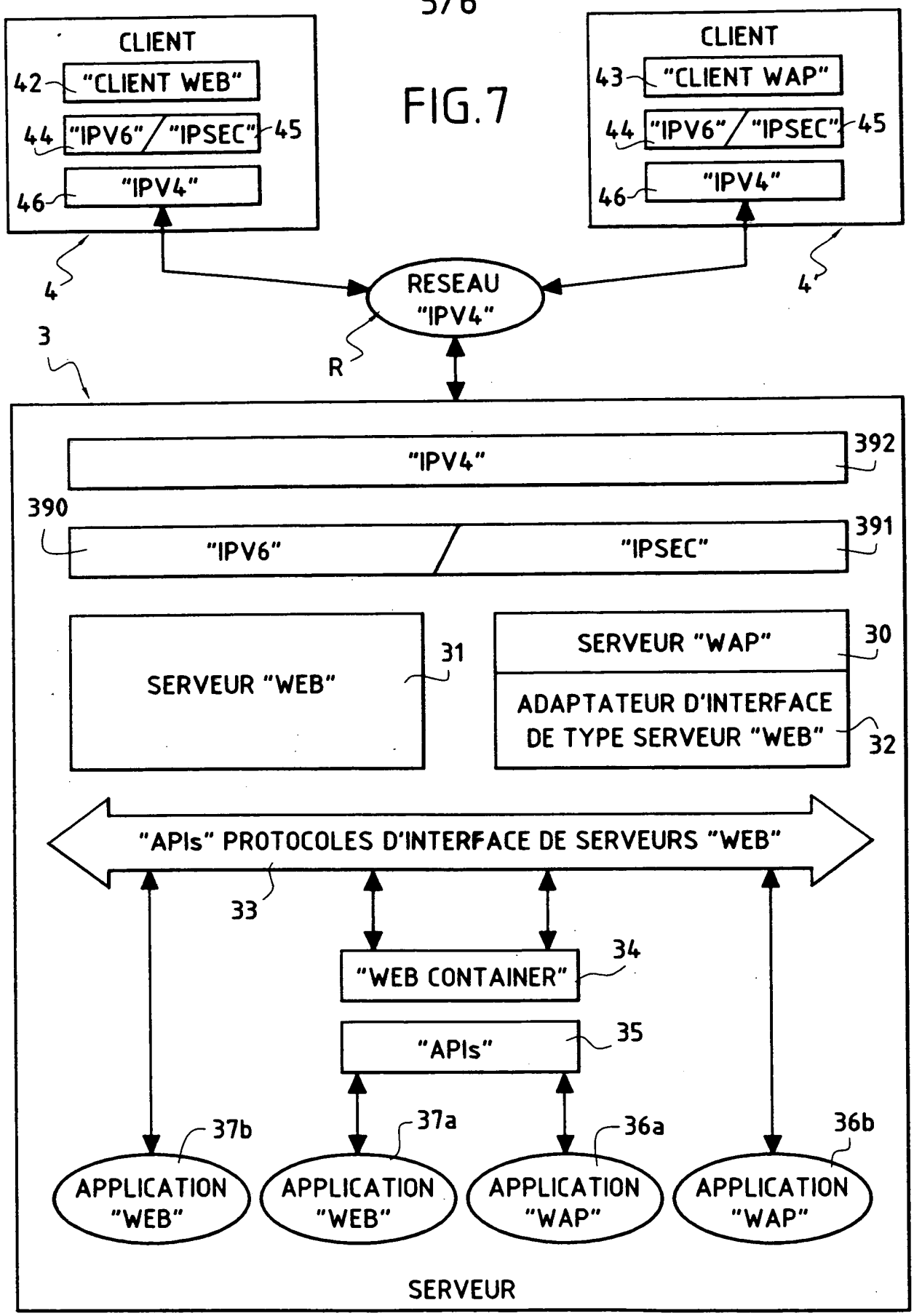
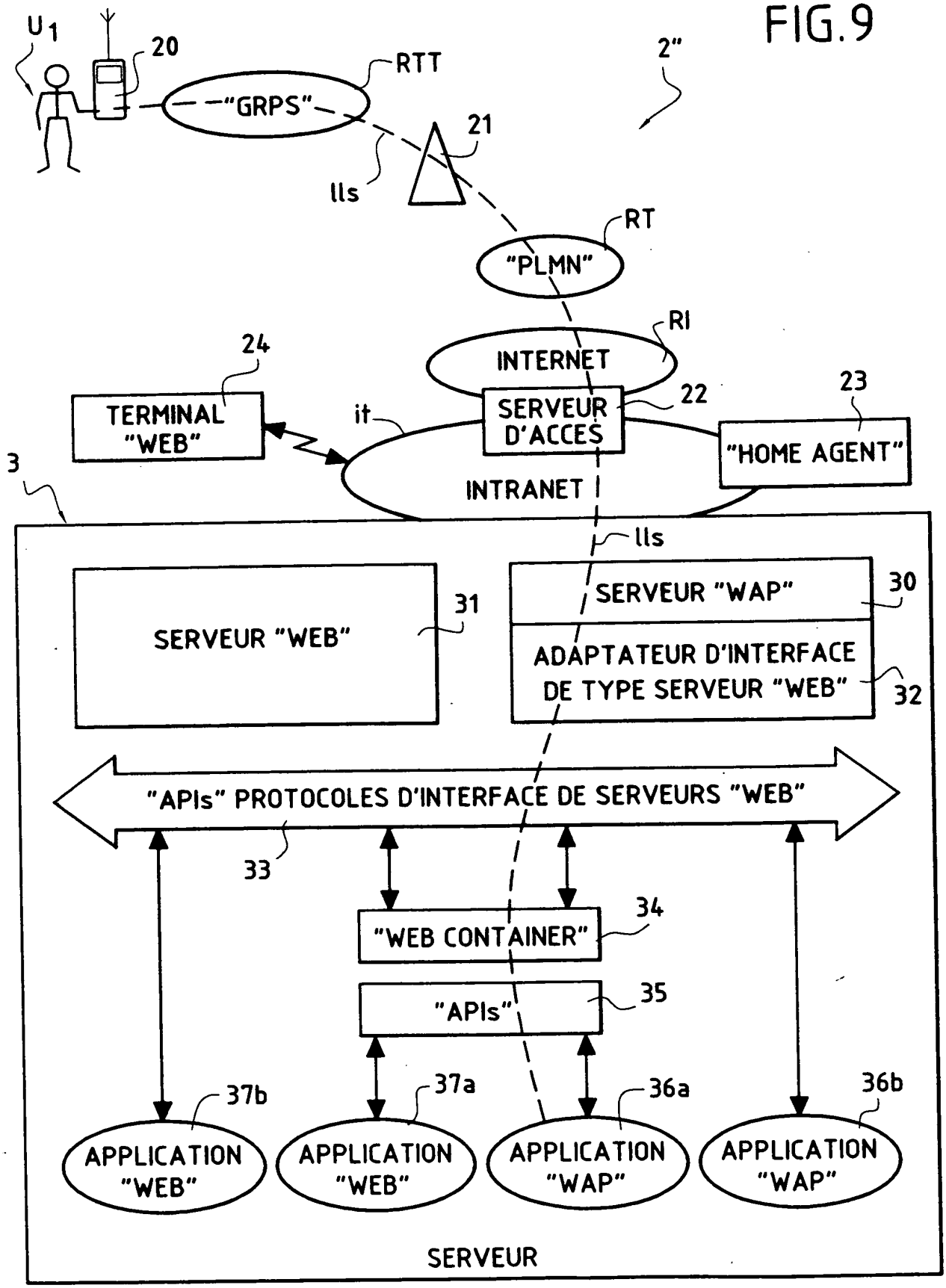

CLIENT
42
"CLIENT WEB"
44
"IPV6"
"IPSEC"
45
46
"IPV4"
CLIENT
43
"CLIENT WAP"
44
"IPV6"
"IPSEC"
45
46
"IPV4"
4
4
RESEAU
"IPV4"
R
3
"IPV4"
392
390
"IPV6"
"IPSEC"
391
SERVEUR "WEB"
31
SERVEUR "WAP"
30
ADAPTATEUR D'INTERFACE
DE TYPE SERVEUR "WEB"
32
"APIs" PROTOCOLES D'INTERFACE DE SERVEURS "WEB"
33
"WEB CONTAINER"
34
"APIs"
35
37b
37a
36a
36b
APPLICATION
"WEB"
APPLICATION
"WEB"
APPLICATION
"WAP"
APPLICATION
"WAP"
SERVEUR

FIG.9


U1
20
"GRPS"
RTT
2"
21
lls
RT
"PLMN"
RI
INTERNET
24
TERMINAL "WEB"
it
SERVEUR D'ACCES
22
23
"HOME AGENT"
3
INTRANET
lls
SERVEUR "WEB"
31
SERVEUR "WAP"
30
ADAPTATEUR D'INTERFACE DE TYPE SERVEUR "WEB"
32
"APIs" PROTOCOLES D'INTERFACE DE SERVEURS "WEB"
33
"WEB CONTAINER"
34
"APIs"
35
37b
37a
36a
36b
APPLICATION "WEB"
APPLICATION "WEB"
APPLICATION "WAP"
APPLICATION "WAP"
SERVEUR